Program Protection

Kristen J. Baldwin
Acting Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))

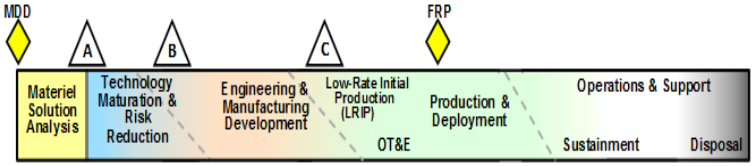
DAU Acquisition Training Symposium
Fort Belvoir, Virginia | April 27, 2016

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Ensuring Cyber Resilience in Defense Systems

- ***Threat:***
  - Adversary who seeks to exploit vulnerabilities to:
    - Acquire program and system information;
    - Disrupt or degrade system performance;
    - Obtain or alter US capability
- ***Vulnerabilities:***
  - Found in programs, organizations, personnel, networks, systems, and supporting systems
  - Inherent weaknesses in hardware and software can be used for malicious purposes
  - Weaknesses in processes can be used to intentionally insert malicious hardware and software
  - Unclassified design information within the supply chain can be aggregated
  - US capability that provides a technological advantage can be lost or sold
- ***Consequences:***
  - Loss of technological advantage
  - System impact – corruption and disruption
  - Mission impact – capability is countered or unable to fight through

Access points are throughout the acquisition lifecycle…



…and across numerous supply chain entry points

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Spectrum of Program Protection Risks to Consider

Quality Escape

inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle

Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion

malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and

Reverse Engineering

Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Information Losses

Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

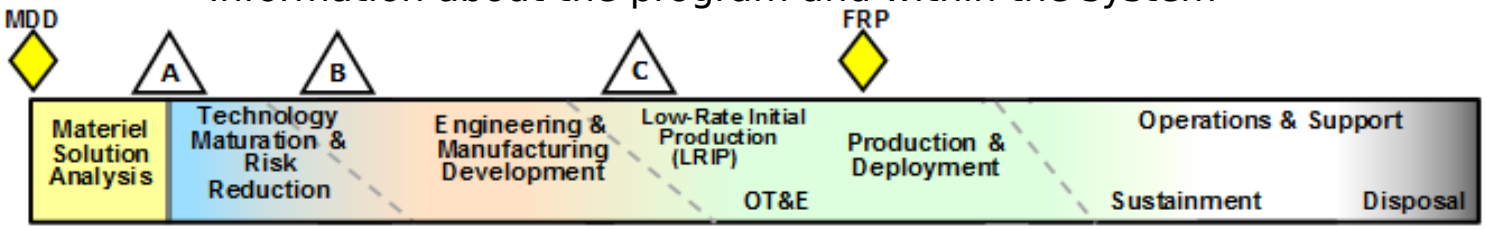
DoD Program Protection focuses on risks posed by malicious actors

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Program Protection in DoDI 5000.02

- **Program Managers, with assistance from supporting organizations, are responsible for protecting the program and the system**

- **DoDI 5000.02 requires program managers to employ system security engineering practices and prepare a Program Protection Plan to manage the security risks to the program and system elements that are vulnerable and can be exposed to targeting**
  - Critical Program Information
  - Mission-critical functions and critical components
  - Information about the program and within the system



Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Cybersecurity in Acquisition

- **Acquisition workforce must take responsibility for the cybersecurity of their programs from earliest research and technology development through system concept, design, development, test and evaluation, production, fielding, sustainment, and disposal**

- **Scope of program cybersecurity includes:**
  - Program information Data about acquisition, personnel, planning, requirements, design, test data and support data for the system. Also includes data that alone might not be unclassified or damaging, but in combination with other information could allow an adversary to compromise, counter, clone, or defeat warfighting capability
  - Organizations and Personnel Government program offices, prime and subcontractors, along with manufacturing, testing, depot and training organizations
  - Networks Government and Government support activities, unclassified and classified networks, contractor unclassified and classified networks, and interfaces among Government and contractor networks
  - Systems and Supporting Systems The system being acquired, system interfaces, and associated training, testing, manufacturing, logistics, maintenance and other support systems

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

What Are We Protecting?

Program Protection & Cybersecurity

DoDI 5000.02 DoDM 5200.01, Vol. 1-4 DoDI 5200.39 DoDI 5200.44 DoDM 5200.45 DoDI 5230.24 DoDI 8500.01 DoDI 8510.01

Technology

What: A capability element that contributes to the warfighters' technical advantage (CPI)

Key Protection Measure Types:
- Anti-Tamper
- Exportability Features

Goal: Prevent the compromise and loss of CPI

Components

What: Mission-critical functions and components

Key Protection Measure Types:
- Software Assurance
- Hardware Assurance/Trusted Microelectronics
- Supply Chain Risk Management
- Anti-counterfeits

Goal: Protect key mission

Information

What: Information about the program, system, designs, processes, capabilities and end-items

Key Protection Measure Types:
- Classification
- Export Controls
- Information Security

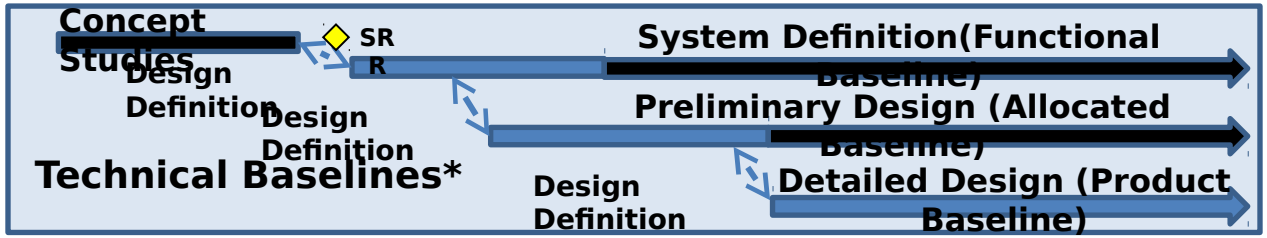
Goal: Ensure key system and program data is protected from adversary

Protecting Warfighting Capability Throughout the Lifecycle

http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Systems Security Engineering Activity Overview



- Protections are identified and integrated into technical baselines
- Analyses are iteratively informed by and informing the design
- Results are documented in the PPP.

Program and System Analyses

SSE Decision Analysis

Contractor

Threat and Vulnerability

Verification & Validation

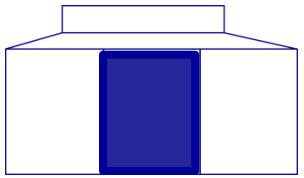
Distribution Statement A – Approved for public ibution is

Anti-Tamper

- AT protects critical program information (CPI) in U.S. systems (those lost/left on the battlefield or exported).
- AT techniques (e.g., hardware protective coatings, software encryption, etc.) may deter, prevent, detect, or respond to an attempt to reverse engineer the system.
- DoD Directive 5200.47E, "Anti-Tamper (AT)," designates the Secretary of the Air Force as the DoD Executive Agent (EA) for AT and assigns responsibilities across the DoD Components for AT protection of CPI.
- The AT Plan, an appendix to the Program Protection Plan, is a document to help develop and communicate a program's AT protection through its lifecycle.
- Programs are encouraged to contact the DoD EA for AT and their Service AT Representative early in the program for guidance.

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Joint Federated Assurance Center



- **JFAC is a federation of DoD software and hardware assurance (SwA/HwA) capabilities and capacities to:**
  - Support programs in addressing current and emerging threats and vulnerabilities
  - Facilitate collaboration across the Department and throughout the lifecycle of acquisition programs
  - Provide SW and HW inspection, detection, analysis, risk assessment, and remediation tools and techniques to PM's to mitigate risk of malicious insertion

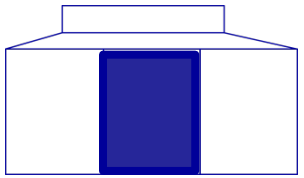
- **JFAC Coordination Center and JFAC Portal**
  - Offers enterprise licenses for SwA tools
  - SwA and HwA best practices, guidance and awareness

- **Lead DoD microelectronic hardware assurance capability providers**
  - Naval Surface Warfare Center Crane
  - Army Aviation & Missile Research Development and Engineering Center

JFAC Portal
https://jfac.army.mil/ (CAC-enabled)

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Trusted Microelectronics Suppliers (e.g. Trusted Foundry)



- **The Defense Microelectronics Activity (DMEA) certifies trusted suppliers for DoD-unique microelectronic designs (e.g. ASIC chips)**
  - There are over 70 trusted suppliers certified by DMEA
- **The IBM Trusted Foundry contract provided microelectronics trust and access for 11+ years to many DoD, intelligence and NASA programs**
  - Broad use by acquisition and technology programs, and special capabilities
  - The IBM TF produced state-of-the-art technology nodes; some of which were IBM-unique
- **GlobalFoundries (GF) acquired IBM's foundry operations in July 2015**
  - In March 2016, DoD awarded a new contract with GF to retain access to the two foundries that provided DoD trusted microelectronics parts
  - **DoD programs are advised to execute life-time buys (LTBs) of production-ready parts while GF Trusted Foundry is available**
- **DoD has established a program to address long term trusted access to microelectronics**
  - Provide an alternative trust model and eliminate reliance on sole source foundries
  - New approach will consist of secure microelectronics design and packaging

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Contract Regulation for Safeguarding Covered Defense Information

DFARS Clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting; 2nd interim rule published December 30, 2015, to provide contractors with additional time to implement NIST 800-171 security requirements. Publication of final rule is planned in the 3rd/4th QTR FY16.

Purpose:

Establish minimum requirements for contractors and subcontractors to safeguard DoD unclassified covered defense information and report cyber incidents on their contractor owned and operated information systems .

Requires Contractors to :

Flow down only to Subcontractors where their efforts will involve covered defense information or where they will provide operationally critical support.

Comply with security requirements in the NIST SP 800-171, "Protecting Controlled Unclassified Information in ***Nonfederal*** Information Systems and Organizations"

Report cyber incident and compromises affecting covered defense information

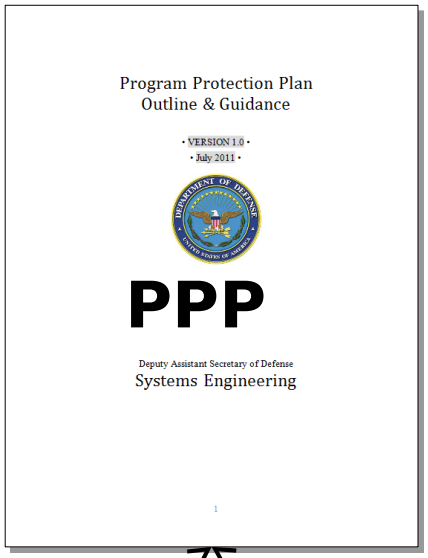
Submit malware that they are able to discover and isolate in connection with a reported cyber incident

Co

The Program Office should pay particular attention to DoD unclassified information provided to, and developed by, the contractor

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Program Protection Relationship to Key Acquisition Activities



SEP

- Incorporation into technical baselines
- SSE entry and exit criteria in SE tech reviews
- SSE as a design consideration
- Technical risks and mitigation plans

TEMP

- Data needed to ascertain cybersecurity requirements are met
- Cooperative Vulnerability Identification and Penetration Assessments

Acq Strat/ Contract

- Trusted supplier requirements
- Acquisition regulations (Safeguarding Covered Defense Information, Counterfeits, etc.)

AT Plan

Cyber-security Strategy/ RMF Security Plan

Tailor to specific program situations

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Intelligence & Counterintelligence Support to Program Protection

- **Effective program protection planning is enabled by intelligence and counterintelligence (CI) support**
  - Threat and CI information can help programs determine what potential protection measures would be most effective for the program's circumstances
  - Program managers should expect to be informed by intelligence and CI throughout the acquisition lifecycle

- **Key information provided by Intelligence and CI sources**
  - Cyber reports
  - Threat reports and assessments
  - Foreign collection methods
  - Suspicious contact reports received from cleared industry
  - Insider threats
  - NISPOM related reporting

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Incorporating Program Protection into Acquisition Workforce Training

- **ACQ 160: Program Protection Overview (est. Summer 2016)**
  - Distance learning (online); ~3 days
  - Provides an overview of program protection concepts, policy and processes
  - Intended for the entire Acquisition Workforce, with focus on ENG and PM

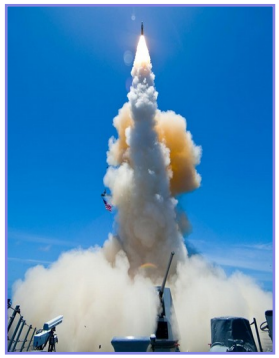
- **ENG 260: Program Protection Practitioner Course (est. Summer 2017)**
  - Hybrid (online and in-class); ~1 week
  - Intended for Systems Engineers and System Security Engineers
  - Focuses on application of program protection concepts and processes

- **Future: Provide topic-specific CLMs**
  - DEE, AT, SwA, SCRM, etc.

Effective program protection planning requires qualified, trained personnel

Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Contact Us

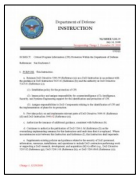


PP/SSE Initiatives Webpage
http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

JFAC Portal
https://jfac.army.mil/ (CAC-enabled)

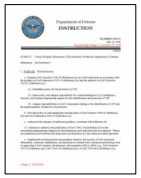
Distribution Statement A – Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

Program Protection Integrated in Policy



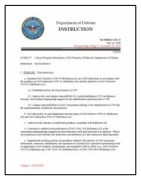
DoDI 5000.02 Operation of the Defense Acquisition System

- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD



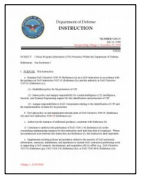
DoDI 5200.39 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)

- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
- Rescoped definition of CPI



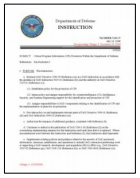
DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components



DoDI 4140.67 DoD Counterfeit Prevention Policy

- Establishes policy and assigns responsibility to prevent the introduction of counterfeit material at any level of the DoD supply chain



DoDI 8500.01 Cybersecurity

- Establishes policy and assigns responsibilities to achieve DoD cybersecurity through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare

Distribution Statement A - Approved for public release by DOPSR case # 16-S-1757. Distribution is unlimited.

DFARS Clause 252.204-7012

	Safeguarding of Unclassified Controlled Technical Information, Nov 18, 2013 *(Final Rule)*	Safeguarding Covered Defense Information and Cyber Incident Reporting, Aug 26, 2015 *(Interim Rule)*	Safeguarding Covered Defense Information and Cyber Incident Reporting, Dec 30, 2015*(Interim Rule)*
Scope – What Information ?	• **Unclassified Controlled Technical Information**	• **Covered Defense Information** • **Operationally Critical Support**	• Covered Defense Information • Operationally Critical Support
Adequate Security – What Minimum Protections ?	• Selected controls in **NIST SP 800-53**, Security and Privacy Controls for **Federal Information Systems** and Organizations	• **NIST SP 800-171,** Protecting Controlled Unclassified Information on **Nonfederal Information Systems** and Organizations	• NIST SP 800-171, Protecting Controlled Unclassified Information on Nonfederal Information Systems and Organizations
When?	• Contract Award	• Contract Award	• As soon as practicable, but **NLT Dec 31, 2017**
When?		**Oct 8, 2015 (Deviation)**	